CLAIMS

What is claimed is:

1. A method of protecting a title key for a recordable media content in a secure distribution system, comprising:

creating an encrypted content/title key package by encrypting the title key with the recordable media content;

transmitting the encrypted content/title key package to a media recording device;

extracting an encrypted title key from the encrypted content/title key package;

obtaining a media key block and a media ID from a physical media;

transmitting the encrypted title key, the media key block, and the media ID to a clearinghouse server utilizing a title key decryption/encryption module;

decrypting the encrypted title key;

deriving a unique media key for the physical media;

creating a re-encrypted title key by encrypting the title key with the unique media key; and

transmitting the re-encrypted title key to the media recording device to record on the physical media with the recordable media content.

2. The method of claim 1, further comprising encrypting the recordable media content with the title key.

3. The method of claim 2, further comprising randomly selecting the title key.

4. The method of claim 2, wherein encrypting the title key comprises encrypting the title key with the recordable media in a manner agreed upon between a recordable media content repository and the clearinghouse server for processing the title key.

5. The method of claim 4, wherein encrypting the title key comprises encrypting the title key with a common key that is agreed upon between the recordable media content repository and the clearinghouse server.

6. The method of claim 4, wherein encrypting the title key comprises encrypting the title key with a public key that is provided by the clearinghouse server.

7. The method of claim 4, wherein encrypting the title key comprises encrypting the title key with a key obtained from a media key block.

8. The method of claim 4, wherein the recordable media content repository stores the encrypted content/title key package for any of sale or distribution to a user.

9. The method of claim 4, further comprising transmitting the encrypted content/title key package to the media recording device.

10. The method of claim 1, further comprising extracting the encrypted title key from the encrypted content/title key package.

11. The method of claim 10, further comprising decrypting the encrypted title key using the media key block and the media ID.

12. The method of claim 11, further comprising deriving a media unique key from the media key block and the media ID.

13. The method of claim 1, further comprising recording the content and the re-encrypted title key on the physical media.

14. The method of claim 1, further comprising transmitting a digest of the media key block to the clearinghouse server instead of a complete media key block.

15. The method of claim 14, further comprising determining from the digest of the media key block whether the media key block has been previously seen.

16. The method of claim 15, further comprising requesting the media key block from the media recording device if the title key decryption/encryption module determines the media key block has not been previously seen.

17. A computer program product having a set of instruction codes for protecting a title key for a recordable media content in a secure distribution system, comprising:

a first set of instruction codes for creating an encrypted content/title key package by encrypting the title key with the recordable media content;

a second set of instruction codes for transmitting the encrypted content/title key package to a media recording device;

a third set of instruction codes for extracting an encrypted title key from the encrypted content/title key package;

a fourth set of instruction codes for obtaining a media key block and a media ID from a physical media;

a fifth set of instruction codes for transmitting the encrypted title key, the

media key block, and the media ID to a clearinghouse server utilizing a title key decryption/encryption module;

a sixth set of instruction codes for decrypting the encrypted title key;

a seventh set of instruction codes for deriving a unique media key for the physical media;

an eight set of instruction codes for creating a re-encrypted title key by encrypting the title key with the unique media key; and

a ninth set of instruction codes for transmitting the re-encrypted title key to the media recording device to record on the physical media with the recordable media content.

18. The computer program product of claim 17, further comprising a tenth set of instruction codes for encrypting the recordable media content with the title key.

19. The computer program product of claim 18, further comprising an eleventh set of instruction codes for randomly selecting the title key.

20. The computer program product of claim 18, wherein the third set of instruction codes encrypts the title key with the recordable media in a manner agreed upon between a recordable media content repository and the clearinghouse server for processing the title key.

21. The computer program product of claim 20, wherein the third set of instruction codes encrypts the title key with a common key that is agreed upon between the recordable media content repository and the clearinghouse server.

22. The computer program product of claim 20, wherein the third set of instruction codes encrypts the title key with a public key that is provided by the clearinghouse server.

23. The computer program product of claim 20, wherein the third set of instruction codes encrypts the title key with a key obtained from a media key block.

24. The computer program product of claim 20, wherein the recordable media content repository stores the encrypted content/title key package for any of sale or distribution to a user.

25. The computer program product of claim 20, further comprising a twelfth set of instruction codes for transmitting the encrypted content/title key package to the media recording device.

26. The computer program product of claim 17, further comprising a thirteenth set of instruction codes for extracting the encrypted title key from the encrypted content/title key package.

27. The computer program product of claim 26, further comprising a fourteenth set of instruction codes for decrypting the encrypted title key using the media key block and the media ID.

28. The computer program product of claim 27, further comprising a fifteenth set of instruction codes for deriving a media unique key from the media key block and the media ID.

29. The computer program product of claim 17, further comprising a sixteenth set of instruction codes for recording the content and the re-encrypted title key on the physical media.

30. The computer program product of claim 17, wherein the sixteenth set of instruction codes further transmits a digest of the media key block to the clearinghouse server instead of a complete media key block.

31. The computer program product of claim 30, further comprising a seventeenth set of instruction codes for determining from the digest of the media key block whether the media key block has been previously seen.

32. The computer program product of claim 31, wherein the seventeenth set of instruction codes requests the media key block from the media recording device if the title key decryption/encryption module determines the media key block has not been previously seen.

33. A system for protecting a title key for a recordable media content in a secure distribution system, comprising:

a content repository server creates an encrypted content/title key package by encrypting the title key with the recordable media content;

the content repository server transmits the encrypted content/title key package to a media recording device;

a title key decryption/encryption module extracts an encrypted title key from the encrypted content/title key package;

the title key decryption/encryption module obtaining a media key block and a media ID from a physical media;

the media recording device transmits the encrypted title key, the media key block, and the media ID to a clearinghouse server by means of the title key

decryption/encryption module;

the clearinghouse server decrypts the encrypted title key and derives a unique media key for the physical media; and

the clearinghouse server then creates a re-encrypted title key by encrypting the title key with the unique media key, and transmits the re-encrypted title key to the media recording device to record on the physical media with the recordable media content.

34. The system of claim 33, wherein the content repository server encrypts the recordable media content with the title key.

35. The system of claim 34, wherein the title key is a randomly selected key.

36. The system of claim 34, wherein the title key is encrypted with the recordable media in a manner agreed upon between a recordable media content repository and the clearinghouse server for processing the title key.

37. The system of claim 36,wherein the title key is encrypted with a common key that is agreed upon between the recordable media content repository and the clearinghouse server.

38. The system of claim 36, wherein the title key is encrypted with a public key that is provided by the clearinghouse server.

39. The system of claim 36, wherein the title key is encrypted with a key obtained from a media key block.

40. The system of claim 36, wherein the content repository server transmits the encrypted content/title key package to the media recording device.